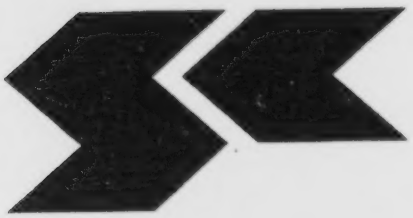
P148597.PDF [Page: 3 of 26]

93-670



DFACTT - SunOS Compartmented Mode Workstation - Security Features Report

Submitted to: Defence Research Establishment Ottawa

Software Kinetics Document No. 1600-116-02 Version 01
Copy #1 05 October 1993

Data Fusion and Correlation Techniques Testbed

(DFACTT)

SunOS Compartmented Mode Workstation (CMW)

Security Features Report

Contract No. W7714-2-9656/01-QC

5 October 1993

Prepared for:

Ms. Janette Hooper
Defence Research Establishment Ottawa
Electronic Warfare Division
Ottawa, Ontario

Prepared by:

Software Kinetics Ltd.
65 Iber Road,
Stittsville, Ontario Canada
K2S 1E7

CAUTION
The use of this information is permitted subject to recognition of proprietary and patent rights.

Software Kinetics Document No. 1600-116-02 *Version* 01

P148597.PDF [Page: 6 of 26]

105-02534/

Document Approval Sheet

Document No.: 1600-116-02 *Version* 01

Document Name: SunOS CMW Security Features Report

Approvals	**Signature**	**Date**
Prepared By:	John E. Derbyshire	1 Nov 93
Project Manager:	John P. Perrin	1 Nov 93

P148597.PDF [Page: 7 of 26]

Document Revision History

Revision	Description of Changes	Origin Date
01	New Document Issued	5 October 1993

P148597.PDF [Page: 8 of 26]

Table of Contents

1. INTRODUCTION 1-1
1.1 Purpose 1-1
1.2 Overview 1-1
1.3 Definitions 1-2
1.4 References 1-2

2. SunOS CMW ARCHITECTURE 2-1
2.1 Application Layer 2-1
2.2 Kernel Layer 2-1
2.3 Hardware Layer 2-1

3. SunOS CMW SECURITY MECHANISMS 3-1
3.1 Secure Windowing Environment 3-1
3.1.1 Cut & Paste and Drag & Drop 3-1
3.1.2 Relabelling Selections During Cut & Paste 3-2
3.1.3 Relabelling Files 3-2
3.2 Identification and Authentication 3-3
3.3 Auditing and Accountability 3-3
3.4 Trusted Path 3-3
3.5 Information and Sensitivity Labels 3-4
3.5.1 Labels on System Entities 3-4
3.5.2 Label Components 3-5
3.5.3 Recognizing Labels 3-6
3.5.4 Relationships Among Labels 3-6
3.5.5 Floating ILs 3-7
3.5.6 Accreditation Ranges 3-7
3.6 Access Control 3-7
3.6.1 Discretionary Access Control (DAC) 3-8
3.6.2 Mandatory Access Control (MAC) 3-8

4. SunOS CMW SYSTEM ADMINISTRATION RESPONSIBILITIES 4-1
4.1 Information System Security Officer 4-1
4.2 System Administrator 4-1
4.3 System Operator 4-1
4.4 Root 4-1

5. SunOS CMW NETWORK SECURITY 5-1
5.1 TCP/IP 5-1
5.2 NFS and Diskless Client Support 5-1
5.3 NIS: Centralized Database Administration 5-1
5.4 Trusted Gateways 5-1
5.5 Interoperability 5-1

APPENDIX I - ACRONYMS AND ABBREVIATIONS I-1

P148597.PDF [Page: 9 of 26]

List of Figures

3-1 SunOS CMW Window System Workspace 3-2
3-2 Screenstripe and Trusted Path Menu 3-4
3-3 Classifications, Compartments and Markings 3-6
3-4 DAC Permission Bits 3-8

P148597.PDF [Page: 10 of 26]

1. INTRODUCTION

1.1 Purpose

The Purpose of this document is to describe the security features of the SunOS Compartmented Mode Workstation (CMW).

1.2 Overview

SunOS CMW is a distributed computer system made up of the SunOS CMW operating system running on one or more Sun machines and servers connected by an Ethernet backbone and administered as a single system. SunOS CMW refers to the system as a whole including the hardware, system software, firmware, documentation and administrative procedures.

SunOS CMW is a secure, multitasking, window-management system that meets the requirements for a compartmented mode workstation as defined in the Security Requirements for System High and Compartmented Mode Workstations, DDS-2600-5502-87 (MTR 9992, Revision 1), November 1991. SunOS CMW also meets the requirements for a B1 level operating system as specified in the "Orange book", or DoD 5200.28-STD, reference [3].

Besides security standards, the SunOS CMW also meets the following industry and government standards:

- X11R4 Windows System
- IEEE Standard 1003.1-1988 (POSIX)
- FIPS 151-1
- X/OPEN XPG2
- System V Interface Definition (SVID) Issue 2 (Vol. 1,2 and 3)
- ABI compatibility with SPARC Compliance Definition 1.0
- MaxSix

SunOS CMW handles classified information at multiple security levels. It uses OpenWindows interfaces to display information at different security levels in separate windows. The data is maintained separately and prevents data of different security levels from being mixed inadvertently or intercepted by "hostile" programs. Classified information can be cut and pasted between windows/files within the boundaries of the security policy. SunOS CMW has a logging capability that is configured by the security officer (referred to in the SunOS CMW literature, reference [1], as the Information System Security Officer (ISSO)). The logging capability can be set up to record

P148597.PDF [Page: 11 of 26]

all security-relevant activities, or to a level required.

A security policy includes a set of rules and practices that regulate how an organization manages, protects and distributes sensitive information. The security features provided by SunOS CMW are only part of the security policy required for the system. The system administrators determine the operations of the security policy, such as physical security of the system and the implementation of optional protection mechanisms.

This document describes the SunOS CMW architecture, security mechanisms, system administrative responsibilities and network security.

1.3 Definitions

Subject - an active entity or process that manipulates data (objects), causes information to flow among objects, or changes the system state. Multiple processes can be run simultaneously, such as an editor, a database manager and an electronic mail program. Each process is a separate entity.

Object - A passive entity that holds or receives information. (ie. a file, a device, a window, a directory or even another process).

Object Re-use - Processes on the system are constantly allocating and re-using objects, such as memory and disk space. SunOS CMW clears all user-accessible objects before allocating them to a process. However, any removable storage medium (floppy disk, tape, etc.) must be cleared before another user can have access to it. Clearing is initiated through device allocation. These media must be kept physically secure and cleared in accordance with local security policy.

1.4 References

[1] SunOS CMW Security Features User's Guide, Sun Microsystems, Inc. Part Number: 800-8939-10, Revision A of December 1992.

[2] Secure Systems for Open Computing - SunOS CMW, Sun Microsystems, September 1991.

[3] Department of Defence Trusted Computer System Evaluation Criteria, DOD 5200.28-STD, US Department of Defence, December 1985.

P148597.PDF [Page: 12 of 26]

2. SunOS CMW ARCHITECTURE

SunOS CMW has the following three layers:

- Application layer
- SunOS CMW kernel layer
- Hardware layer

2.1 Application Layer

The application layer includes all the commands, libraries and utility programs used to operate the system including the OpenWindows environment. The windowing environment includes the following security features:

- Screenstripe - displays information label of the keyboard and the information label and sensitivity label of the application that contains the mouse pointer.
- Trusted Path menu for security related commands.
- Management of cut-and-paste data between windows.
- Management of the user workspace.
- Deskset tools at differing security levels.

2.2 Kernel Layer

The kernel controls the hardware and performs low-level services such as managing the file system, processes, and system resources. SunOS CMW retains most of the functionality of standard SunOS, however, some functions have been modified or removed to meet security needs of compartmented mode operation. There have also been some system security additions to the Operating System (OS) such as, auditing, file-access control, sensitivity labels, information labels and privileges.

2.3 Hardware Layer

The hardware layer consists of the physical components of the system including the computer, disk drives, tape drives, monitor, keyboard, mouse and network. Protection of the hardware is managed by a physical security policy specific to each location or use.

P148597.PDF [Page: 13 of 26]

3. SunOS CMW SECURITY MECHANISMS

SunOS CMW uses protection mechanisms implemented on a base of hardware, firmware and software to achieve security. SunOS CMW includes the following security mechanisms:

- Secure windowing environment to prevent unintentionally compromising the integrity of data.
- User identification and authentication to prevent unauthorized penetration of the system.
- Auditing user actions and system events provides accountability.
- Trusted path mechanism to ensure users are not "spoofed" by hostile programs.
- Information and sensitivity labelling of classified information to allow access control.
- Access control on files, directories, processes and devices provides control based on the security policy and on a need-to-know basis.

3.1 Secure Windowing Environment

The user interacts with SunOS CMW through the multi-level secure window system that is based on Sun's OpenWindows. The label of each window is displayed in a banner which is colour coded to match the sensitivity label. The labelling system and trusted path mechanism ensure that security is maintained while allowing the following features:

- Cut & Paste and Drag & Drop
- Relabelling Selections During Cut & Paste
- Relabelling Files

Figure 3-1 shows a typical SunOS CMW window display consisting of a workspace, windows, menus, icons and a screenstripe.

3.1.1 Cut & Paste and Drag & Drop

SunOS CMW allows users to cut and paste or drag and drop between windows. All such transfers are mediated by a trusted selection agent. This tool supports transfer of text, binary data and graphics between windows. The window system prevents unauthorized transfers, and makes it possible for the security officer to audit successful and failed transfers.

During cut and paste operations between windows, the user must confirm the transfer. During certain operations, such as those in which the source and destination files labels are equal, the user can configure the system to automatically confirm the transfer.

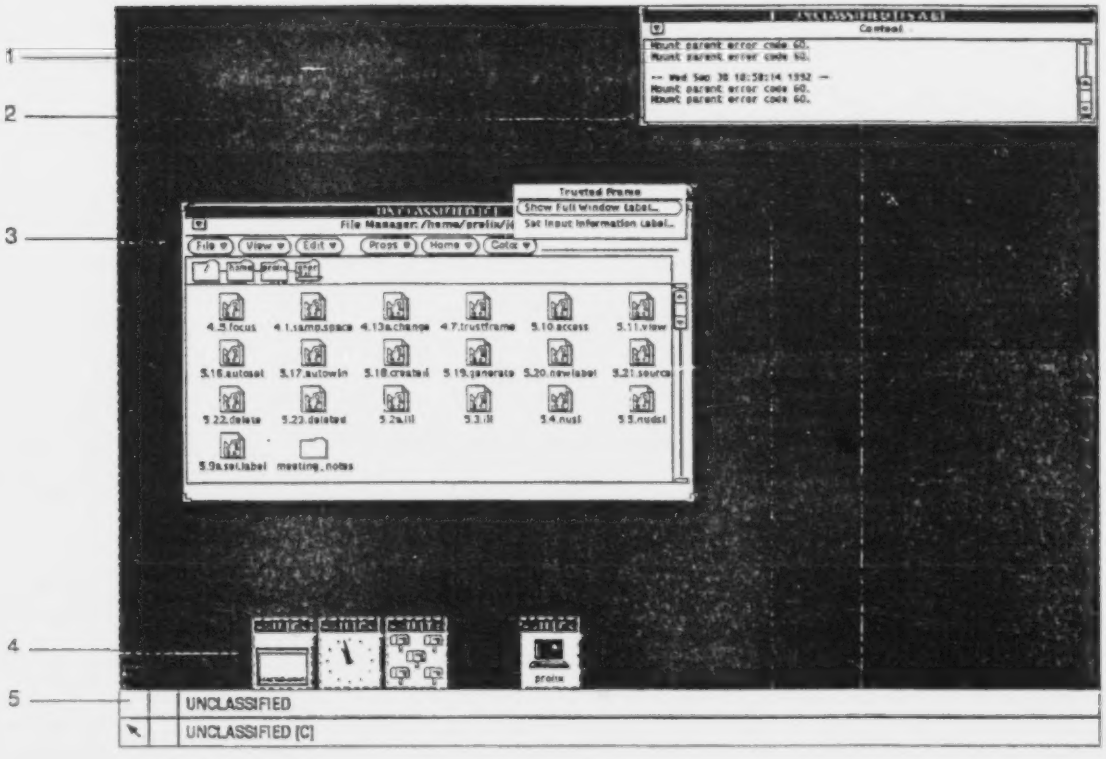
P148597.PDF [Page: 14 of 26]

3.1.2 Relabelling Selections During Cut & Paste

During cut and paste operations, before confirming a transfer, the user can view the selected data and change its sensitivity label. If the user is given the appropriate authorization from the security officer, the user may also upgrade or downgrade the sensitivity of data during a transfer.

3.1.3 Relabelling Files

Files can be relabelled by drag and drop from the File Manager into the Trusted File Labeller. A user who has been authorized by the security officer can lock a file and view it in a trusted window before relabelling the information or sensitivity label.



1 - Workspace 2 - Window 3 - Menu 4 - Icon 5 - Screenstripe

Figure 3-1 SunOS CMW Window System Workspace

P148597.PDF [Page: 15 of 26]

3.2 Identification and Authentication

The login process is one of identification and authentication. To log in, the user name and password are entered as is normal for a Unix based system. After log in, a process is created for the user. This process and all other processes acting for that user inherit the user identification (ID), which indicates ownership of the process. Objects such as files, have an owner ID which is set to the user ID of the user that creates the object.

System administrators can configure the system to require a system-generated password and also determine how long a password is valid.

3.3 Auditing and Accountability

SunOS CMW ensures accountability through the identification and authorization that is performed during login and during the assumption of trusted roles. Accountability is also ensured through the auditing of system events. Each system event can be recorded in an audit record. The audit transaction can log the event, the date and time, the user and the success or failure of the event. The ISSO controls which events are audited.

Auditing allows for the reconstruction of actions by a user and for evaluation of all activities. Auditing can monitor for attempts to compromise the security of the system and can be used to determine the extent to which the system was penetrated.

3.4 Trusted Path

The trusted path mechanism provides a trustworthy means for users to interact with security-critical operations such as during log in, and any other operations that require users to enter their password or to enter a sensitivity or information label. It incorporates features that identify trusted path activity to ensure that users are not "spoofed" by hostile programs.

Users access the trusted path menu from the trusted screenstripe. All security-relevant programs are started from the trusted path menu, which can not be interfered with by untrusted programs. Authorized users assume their administrative roles and access administrative menus from the trusted path menu. The screenstripe can never be obscured by untrusted programs and therefore will always display the correct information. When a trusted path application is active, the screenstripe displays the trusted shield (a triangle apex downwards with a "T" in the centre), see figure 3-2.

The trusted path interface prevents "trojan horse", and misleading programs that surreptitiously exploit security and integrity.

P148597.PDF [Page: 16 of 26]

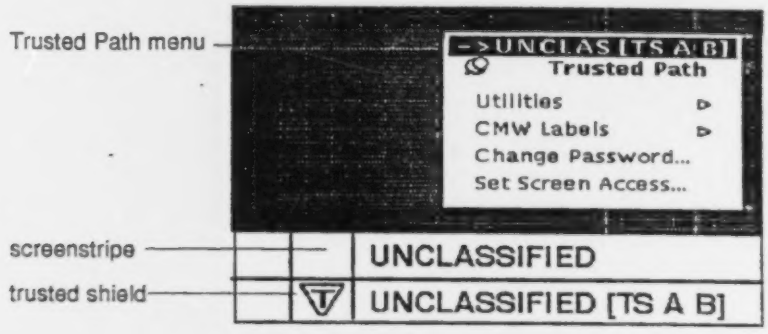


Figure 3-2 Screenstripe and Trusted Path Menu

3.5 Information and Sensitivity Labels

Labels represent levels of security. SunOS CMW assigns labels to subjects and objects to regulate the flow of information. A label has two components: an Information Label (IL) and a Sensitivity Label (SL).

- A SL describes the security level at which a subject or object is protected by the mandatory access control policy. The SL usually reflects the classification of the subject that creates the object.

- An IL describes the security level of the information contained within a subject or an object as well as markings and caveats.

In most circumstances, SLs are inherited and do not change whereas ILs float (move up).

3.5.1 Labels on System Entities

SunOS CMW assigns labels to each of the following system entities:

Processes - Process Labels

Each process has a SL and an IL. On log in, the user default SL and the default SLs of all user processes are the ISSO-assigned SL of the user home directory. The default SL sets the lower boundary of the range of labels in which the user can operate. The IL of a process represents the label of information contained by the process. When a process reads a data object, the IL of the data object floats up to the IL of the process. When a process writes to a data object, the process IL may float up to the IL of the data.

Files - File Labels

Each file has a SL and an IL. When created, a file is assigned the same SL as the creating process. When a file is empty and contains no information, it is initialized to an IL of SYSTEM_LOW.

P148597.PDF [Page: 17 of 26]

Directories - Directory Labels

There are two types of directories, single label and multi-label. The user home directory is a single label directory that is set to the lowest label allowed to the user. From the home directory, a user can create directories at higher levels. Multi-label directories are used by files like /tmp that contain files with different SLs.

Devices - Device Labels

Devices are also subject to mandatory access control. Each device has an upper and lower level of sensitivity. These levels determine the range of SLs that have access to that device.

Input information - Input Information Label

The Input Information Label (IIL) is a label, displayed in the screenstripe, that SunOS CMW associates with each window. The IIL specifies the label of the data entered from the keyboard and mouse. The IIL can be changed at any time.

3.5.2 Label Components

SLs and ILs contain hierarchical and nonhierarchical elements: classification and compartments. ILs can also contain security markings. Figure 3-3 shows the relationship between classifications, compartments and markings.

Classifications

Classifications represent hierarchical levels of security. Each label has one classification of the possible 16 classifications supported by SunOS CMW.

Compartments

Compartments are nonhierarchical and are independent of classifications. Compartments usually are used to represent work groups, projects or topics. e.g. A label with the classification SECRET might include the compartments DFACTT and ACES. A label with the classification UNCLASSIFIED might also have the same compartments. SunOS CMW supports a maximum of 128 compartments

Markings

ILs contain a set of nonhierarchical markings. Markings describe special handling instructions for information. e.g. EYES ONLY, LIMDIS (limited distribution), NOFORN (no foreign distribution). SunOS CMW supports a maximum of 128 markings.

P148597.PDF [Page: 18 of 26]

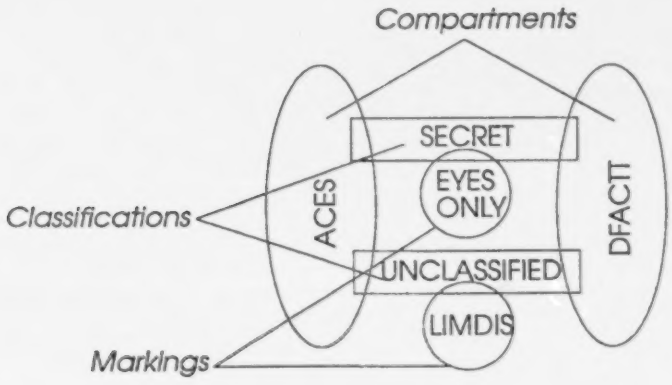


Figure 3-3 Classifications, Compartments and Markings

3.5.3 Recognizing Labels

A label is represented by a string consisting of the classification, the compartment and the markings. Label components can appear in full or in abbreviated format. e.g. Consider a file containing secret information on the DFACTT project in the Analyst group. The classification on the file is SECRET, the compartments include DFACTT and ANALYST. The file label is SECRET DFACTT ANALYST with the short form S DT AT.

Note: The label_encodings file defines labels configured for the SunOS CMW system. At installation, an ISSO can modify the default file to specify the labels, clearances, and the system and user accreditation ranges for the site. Modifying the label_encodings file after installation will result in problems.

3.5.4 Relationships Among Labels

SunOS CMW defines the mandatory access control security policy in terms of label dominance, equality, and disjunction. Whether a subject can access an object depends on whether the subject label dominates the object label, equals it or is disjoint from it.

Dominance

A label x dominates anther label y if all of the following are true::

- classification of x >= classification y
- The set of compartments of x includes all the compartments of y
- If x and y are ILs, the set of markings of x include all markings of y

P148597.PDF [Page: 19 of 26]

Equality

If label x and label y have the same component parts, x is equal to y if the following are both true:

- All components are identical
- x dominates y and y dominates x

Note: If one of the two labels included a compartment or a marking that the other does not, the labels are not equal.

Disjunction

If x and y are labels, they are disjoint or not comparable if neither one dominates the other. e.g. SECRET DFACTT and CONFIDENTIAL ACES are disjoint labels.

3.5.5 Floating ILs

ILs are often combined together to form a third IL. This combination is the arithmetic maximum of the classification portion of the labels, and the union of the compartment and marking portions of the labels. Often the merging of two ILs tends to increase the classification while the compartment and marking sets accumulate additional elements. In such situations, the ILs are said to float up.

3.5.6 Accreditation Ranges

System accreditation range is the set of SLs that include the valid sensitivity labels on each machine, defined by the limits of SYSTEM_LOW and SYSTEM_HIGH. SYSTEM_LOW is the label which is dominated by all other labels, and SYSTEM_HIGH dominates all other labels.

The user accreditation range defines the limits in which a user can create processes. Each process created by a user is assigned a SL within the user accreditation range and dominated by the user's clearance.

The user accreditation range does not include SYSTEM_LOW and SYSTEM_HIGH but the system accreditation range does. The SYSTEM_HIGH label protects system files that should not be read or altered by users. SYSTEM_LOW protects public executables such as those that are part of the standard Sun software and those that are part of the trusted computing base. Since a user cannot run at SYSTEM_LOW, the user can read these executable files but cannot write to them.

3.6 Access Control

Access control to sensitive information is accomplished through Discretionary Access Control (DAC) and Mandatory Access Control (MAC). Access based on identity and need-to-know is governed by standard UNIX DAC that has been incorporated into SunOS CMW. Access based on the SL of a subject or an object is granted by MAC. Both the requirements of DAC and MAC must be satisfied to gain access to an object.

P148597.PDF [Page: 20 of 26]

3.6.1 Discretionary Access Control (DAC)

DAC restricts access to objects based on the user identity or group membership. DAC is implemented, as for standard UNIX, through permission bits for the owner, the group and the world. A user that creates an object is the owner of that object and can therefore assign DAC permissions for the object. Figure 3-4 shows how the DAC permission bits are represented in a directory listing.

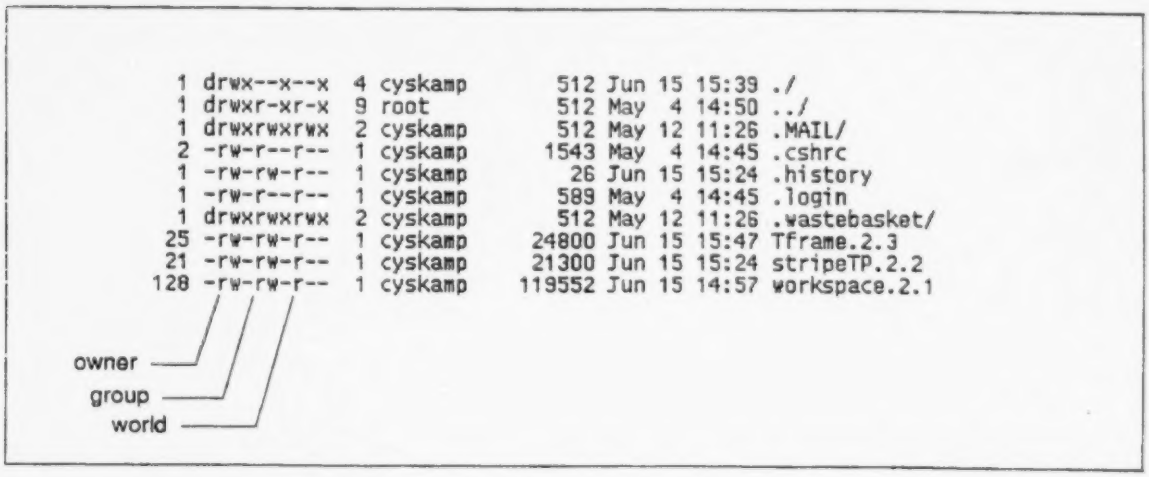

1 drwx--x--x 4 cyskamp 512 Jun 15 15:39 ./
1 drwxr-xr-x 9 root 512 May 4 14:50 ../
1 drwxrwxrwx 2 cyskamp 512 May 12 11:26 .MAIL/
2 -rw-r--r-- 1 cyskamp 1543 May 4 14:45 .cshrc
1 -rw-rw-r-- 1 cyskamp 26 Jun 15 15:24 .history
1 -rw-r--r-- 1 cyskamp 589 May 4 14:45 .login
1 drwxrwxrwx 2 cyskamp 512 May 12 11:26 .wastebasket/
25 -rw-rw-r-- 1 cyskamp 24800 Jun 15 15:47 Tframe.2.3
21 -rw-rw-r-- 1 cyskamp 21300 Jun 15 15:24 stripeTP.2.2
128 -rw-rw-r-- 1 cyskamp 119552 Jun 15 14:57 workspace.2.1
owner
group
world

Figure 3-4 DAC Permission Bits

3.6.2 Mandatory Access Control (MAC)

MAC is used with DAC to control access to system files. MAC is based on SLs that are used to prevent compromise of sensitive information. Sensitivity labelling imposes a systemwide, centralized security policy on all users and system activities. Since both MAC and DAC control access to information, DAC restrictions must still be satisfied even when MAC criteria are satisfied. The following describe the MAC criteria for access to information:

- Read access requires that the subject SL dominate the object SL. i.e., The process SL must dominate the data file SL in order for the process to read the data.
- Write access requires that the subject SL be dominated by the object SL. i.e., The SL of a file must dominate the SL of a process in order for the process to write to the file.
- Combined read/write access requires equality between the subject SL and the object SL.

P148597.PDF [Page: 21 of 26]

4. SunOS CMW SYSTEM ADMINISTRATION RESPONSIBILITIES

The SunOS CMW system administrative responsibilities are divided into the following four Trusted Facilities Management (TFM) roles, each with its own authorization requirements:

- Information System Security Officer (ISSO)
- System Administrator
- System Operator
- Root role

The system requires the ISSO, the system administrator and the system operator in order to properly administer the secure system.

4.1 Information System Security Officer

The ISSO responsibilities include assigning clearance, authorizations, initial passwords, password duration for users and changing SLs and ILs on objects. The ISSO is the most security sensitive role.

4.2 System Administrator

The system administrator performs most of the normal administration tasks such as adding or modifying user accounts. The system administrator also assigns the ISSO authorization.

4.3 System Operator

The system operator handles the day-to-day operations of the system, such as backups.

4.4 Root

For special situations where the ISSO cannot install certain applications because the installation requires a user ID of 0, the ISSO can assume the root role to perform the installation.

P148597.PDF [Page: 22 of 26]

5. SunOS CMW NETWORK SECURITY

SunOS CMW treats the system of workstations and servers linked together as a single security environment. It makes available the networking features of open systems with the B1 and CMW security protection.

5.1 TCP/IP

Trusted versions of the standard TCP/IP mechanisms are able to pass along the security attributes of the connection or the transmitted data. The standard interfaces are preserved by allowing existing applications to operate without modification. New interfaces obtain the security attributes of the information being transferred between machines, while enforcing mandatory access controls.

5.2 NFS and Diskless Client Support

The SunOS CMW implementation of NFS, the standard Sun distributed file sharing facility, provides transparent access to remote files while enforcing the mandatory and discretionary access controls and propagating CMW security attributes. The operation of diskless client machines is fully supported using NFS. Exporting and importing of file systems to and from single level non-CMW machines is also supported in a trusted manner.

5.3 NIS: Centralized Database Administration

The Network Information Service (NIS) is fully operational in SunOS CMW and protected by the privilege mechanism from unauthorized access. NIS centralizes storage and maintenance of system-wide configuration data.

5.4 Trusted Gateways

SunOS CMW provides both multi-level and single-level gateway capabilities. This allows sites to connect their distributed system with other networks at a configurable level of trust and with propagation of security attributes.

5.5 Interoperability

Interoperability between SunOS CMW and other secure OSs is supported through the MaxSix trusted network protocols. In addition, interoperability with commercial, non-CMW systems is supported through a single-level host mechanism

P148597.PDF [Page: 23 of 26]

APPENDIX I - ACRONYMS AND ABBREVIATIONS

CMW	Compartmented Mode Workstation
DAC	Discretionary Access Control
DFACTT	Data Fusion and Correlation Techniques Testbed
ID	Identification
IIL	Input Information Label
IL	Information Label
ISSO	Information System Security Officer
LIMDIS	Limited Distribution
MAC	Mandatory Access Control
NFS	Network File Service
NIS	Network Information Service
NOFORN	No Foreign Distribution
OS	Operating System
SL	Sensitivity Label
TFM	Trusted Facilities Management

P148597.PDF [Page: 24 of 26]

SECURITY CLASSIFICATION OF FORM
(highest classification of Title, Abstract, Keywords)

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Software Kinetics Ltd.
65 Iber Road
Stittsville, Ont.

2. SECURITY CLASSIFICATION (overall security classification of the document including special warning terms if applicable)

Unclassified

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

DFACTT SUN OS Compartmented Mode Workstation (CMW) Security Features Report

4. AUTHORS (Last name, first name, middle initial)

Derbyshire, John E.
Perrin, John P.

5. DATE OF PUBLICATION (month and year of publication of document)

October 1993

6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)

14

6b. NO. OF REFS (total cited in document)

3

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Report

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

Defence Research Establishment Ottawa
Shirleys Bay

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant)

Data Fusion and Correlation
Techniques Testbed

9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)

W77 14-2-9656/01-QC

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)

1600-116-02 Version 01

10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)

None

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(X) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors; further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

Unannounced

P143597.PDF [Page: 25 of 26]

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both offical languages unless the text is bilingual).

The report provided an overview of the Sun OS Compartmented Mode Workstation Environment. It describes the CMW architecture, security mechanisms, administration responsibilities and network security.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Security

Secure Operating System

Compartmented Mode Workstation

Trusted Platform

Information Security

TITLE:(U) DATA FUSION AND CORRELATION TECHNIQUES TESTBED (DFACTT) - SUNOS COMPARTMENTED MODE WORKSTATION (CMW) - SECURITY FEATURES REPORT

PERSONAL AUTHOR: Derbyshire, J.E.
CORPORATE AUTHOR: Software Kinetics Ltd, Stittsville ONT (CAN);Defence Research Establishment Ottawa, Ottawa ONT (CAN)

ABSTRACT: (U) Provides an overview of the Sun OS Compartmented Mode Workstation Environment. It describes the CMW architecture, security mechanisms, administration responsibilities and network security.

DESCRIPTORS: (U) WORKSTATIONS;COMPUTER NETWORKS;DATA PROCESSING SECURITY;SECURE COMMUNICATION;COMPUTERS;COMPUTER ARCHITECTURE;OPERATING SYSTEMS (COMPUTERS)
IDENTIFIERS: (U) COMPARTMENTED MODE WORKSTATION;TRUSTED PLATFORM

REPORT NUMBER: SKD-1600-116-02;DREO-CR-93-670; Contractor Report
REPORT DATE: 05 Oct 1993
NUMBER OF PAGES : 23
DRDKIM N°: 95-01216
CANDIS N°: 148597
Format(s): Hardcopy;Document Image stored on Optical Disk

It is recommended you search "Authors" and "Corporate Authors" on their respective "Browse" pages.

Click here if you are having problems displaying text (ie. text is too big, or too small) or page appears to be jumbled.

Date modified: 2003-04-17 Important Notices